On the Performance of Sphere Decoding of Block Codes.

Mostafa El-Khamy, Haris Vikalo, Babak Hassibi and R. J. McEliece
Electrical Engineering Department
California Institute of Technology
Pasadena, CA 91125, USA
E-mail: mostafa, hvikalo, hassibi, rjm@systems.caltech.edu

***Abstract*— The performance of sphere decoding of block codes over a variety of channels is investigated. We derive a tight bound on the performance of maximum likelihood decoding of linear codes on q-ary symmetric channels. We use this result to bound the performance of q-ary hard decision sphere decoders. We also derive a tight bound on the performance of soft decision sphere decoders on the AWGN channel for BPSK and M-PSK modulated block codes. The performance of soft decision sphere decoding of arbitrary finite lattices or block codes is also analyzed.**

I. Introduction and Summary

A maximum likelihood decoder returns the closest codeword or lattice point to the received vector. Fincke and Pohst [1] developed a *sphere decoder* to solve the closest-point problem in general lattices.[2]. A faster sphere decoding algorithm was given by Schnorr and Euchner [3]. Algorithms based on sphere decoders are currently the state of the art for decoding and detection in multiple input multiple output linear channels [4], [5], [6]. One can also think of the Guruswami-Sudan (GS) decoder [7] as a sphere decoder for Reed Solomon (RS) codes whose radius can be larger than half the minimum distance. The radius of the sphere decoder provides a tradeoff between performance and complexity.

The performance of sphere decoding of linear block codes on additive white Gaussian noise channels (AWGN) and binary symmetric channels (BSC) was analyzed in our previous work [8]. In this paper, we analyze the performance of linear block codes, defined over F_q, when transmitted over q-ary symmetric channels (QSC) and the decoder is either the maximum likelihood decoder or a sphere decoder with an arbitrary search radius. This is done in Sec. II. These results are used to analyze the performance of RS codes on q-ary symmetric channels. In Sec. III, we derive tight bounds on the performance of sphere decoding of linear block codes with a binary or M-ary PSK modulation over an AWGN channel. We then show, in Sec. IV, how the performance of sphere decoding of an arbitrary code with an arbitrary modulation scheme (finite lattice) on AWGN channels can be analyzed. We illustrate the tightness of our analytic bounds by comparing them to numerical simulations.

II. Sphere Decoding of Codes in F_q Over q-ary Symmetric Channels.

Consider an (n, k, d) linear code $\mathcal{C}$ over the finite field of q elements, F_q, transmitted over a q-ary symmetric channel (QSC) and a sphere decoder which can correct τ symbol errors, where the symbols are in F_q. For the case of RS codes, the GS algorithm can correct up to $\tau_{GS} = \lceil n - \sqrt{nk} - 1 \rceil$ symbol errors which is at least as big as the radius of the conventional Berlekamp-Massey algorithm, $\tau_{BM} = \lfloor \frac{n-k}{2} \rfloor$. The bounded distance decoder error probability of RS codes has been previously studied (e.g. [9]).

Let s and $p = (1-s)/(q-1)$ denote the success and error crossover probabilities of the QSC respectively. Transmitting a q-ary code over an AWGN channel followed by hard-decision can be modeled as transmitting it over an QSC. Assume that $q = 2^m$, the channel alphabet size is 2^b, $b \leq m$, and each q-ary symbol is mapped to m/b channel symbols. Let p_c be the probability that a channel symbol is incorrectly decoded, then $s = (1-p_c)^{m/b}$.

A. Bound on the ML decoding of linear block codes on q-ary symmetric channels.

Let ζ be the Hamming distance between the transmitted codeword and the received word in F_q^n. Throughout this paper $\mathcal{E}_{ML}$ will denote the event of an ML error. Then, similar to the binary case [10], the ML error probability can be upper bounded as follows,

$$P(\mathcal{E}_{ML}) \leq \min_m \left\{ P(\mathcal{E}_{ML}, \zeta < m) + P(\zeta \geq m) \right\}. \quad (1)$$

Assuming that the code is linear, the probability that the received q-ary word lies outside a Hamming sphere (ball) of radius $m-1$ centered around the transmitted word is

$$P(\zeta \geq m) = \sum_{\alpha=m}^{n} \binom{n}{\alpha} (1-s)^{\alpha} s^{n-\alpha}. \quad (2)$$

The above equation will also provide a lower bound on the performance of the sphere decoder. The first term in (1) is upper bounded in the following lemma.

Lemma 1: For an (n, k, d) linear code over F_q, with a weight enumerator G_w, transmitted over a q-ary symmetric

channel with parameters s and p,

$$P(\mathcal{E}_{ML}, \zeta < m) \leq \sum_{w=d}^{\min\{n,2(m-1)\}} G_w \sum_{\alpha=0}^{\min\{w,m-1\}} \sum_{\eta=\lceil \frac{w-\alpha}{2} \rceil}^{w-\alpha} \left(\frac{w!}{\eta!\alpha!(w-\eta-\alpha)!} p^{\eta}(1-p-s)^{\alpha} s^{w-\eta-\alpha} \sum_{\beta=0}^{m-1-\eta-\alpha} \binom{n-w}{\beta} (1-s)^{\beta} s^{n-w-\beta} \right). \quad (3)$$

Proof: We will assume that the all-zero codeword is transmitted. Now consider a codeword $\boldsymbol{c}$ with Hamming weight w and assume the received word $\boldsymbol{r}$ has a Hamming weight $m'-1$. Consider the w nonzero symbols in $\boldsymbol{c}$ and the corresponding coordinates in $\boldsymbol{r}$. Let $\boldsymbol{r}$ and $\boldsymbol{c}$ have the same symbols in η of these coordinates. Let α of these w coordinates in $\boldsymbol{r}$ be neither zero nor match those in $\boldsymbol{c}$, and $w-\eta-\alpha$ of the remaining coordinates be zero. Since the Hamming weight of $\boldsymbol{r}$ is $m'-1$, there must be $m'-1-\eta-\alpha$ non-zero symbols in the remaining $n-w$ coordinates and the remaining symbols will be zero. The probability of receiving such a word is $\frac{w!}{\eta!\alpha!(w-\eta-\alpha)!} p^{\eta}(1-p-s)^{\alpha} s^{w-\eta-\alpha} \binom{n-w}{m'-1-\eta-\alpha} (1-s)^{m'-1-\eta-\alpha} s^{n-w-(m'-1-\eta-\alpha)}$. In such a case, the Hamming distance between $\boldsymbol{r}$ and $\boldsymbol{c}$ is $w+m'-1-2\eta-\alpha$. An ML error results if this is less than the weight of $\boldsymbol{r}$, i.e., if $\eta \geq \lceil \frac{w-\alpha}{2} \rceil$. By summing over all possible combinations of η and α and applying the union bound for all codewords that can be within a Hamming distance m' from $\boldsymbol{r}$, the error probability is upper bounded by $\sum_{w=d}^{2(m'-1)} G_w \sum_{\alpha=0}^{m'-1} \sum_{\eta=\lceil \frac{w-\alpha}{2} \rceil}^{w-\alpha} \left(\frac{w!}{\eta!\alpha!(w-\eta-\alpha)!} p^{\eta}(1-p-s)^{\alpha} s^{w-\eta-\alpha} \binom{n-w}{m'-1-\eta-\alpha} (1-s)^{m'-1-\eta-\alpha} s^{n-w-(m'-1-\eta-\alpha)} \right)$. Applying the union bound for all received words with Hamming weights less than m, $m' \leq m$, the result follows. ■

One can now prove the following theorem,

Theorem 2: The ML error probability of an (n,k,d) q-ary linear code on a q-ary symmetric channel is upper bounded by

$$P(\mathcal{E}_{ML}) \leq \sum_{w=d}^{\min\{n,2(m_o-1)\}} G_w \sum_{\alpha=0}^{\min\{w,m_o-1\}} \sum_{\eta=\lceil \frac{w-\alpha}{2} \rceil}^{w-\alpha} \left(\frac{w!}{\eta!\alpha!(w-\eta-\alpha)!} p^{\eta}(1-p-s)^{\alpha} s^{w-\eta-\alpha} \sum_{\beta=0}^{m_o-1-\eta-\alpha} \binom{n-w}{\beta} (1-s)^{\beta} s^{n-w-\beta} \right) + \sum_{\alpha=m_o}^{n} \binom{n}{\alpha} (1-s)^{\alpha} s^{n-\alpha},$$

where m_o is the smallest integer m such that

$$\sum_{w=d}^{\min\{n,2m\}} G_w \sum_{\alpha=0}^{\min\{w,m\}} \left(\frac{q-2}{q-1} \right)^{\alpha} \sum_{\eta=\lceil \frac{w-\alpha}{2} \rceil}^{w-\alpha} \left(\frac{1}{q-1} \right)^{\eta} \frac{w!}{\eta!\alpha!(w-\eta-\alpha)!} \binom{n-w}{m-\eta-\alpha} \geq \binom{n}{m}. \quad (4)$$

It is worth noting that the optimum radius m_o which minimizes the bound on the ML error probability only depends on the weight enumerator of the code and the size of its finite field. Since the optimum radius does not depend on the SNR, it is valid for q-ary symmetric channels at any SNR. We also establish below a connection between m_o and the covering radius of the code.

Lemma 3: The covering radius of a linear code on F_q is lower bounded by $m_o - 1$, where m_o is given by Th. 2.

Proof: Define $L(m)$ to be the left hand side term in (4) and $\boldsymbol{c}_o$ to be the all zero codeword. Similar to the proof of Lem. 1, one can show that $(q-1)^m L(m) = |\{\boldsymbol{r} \in F_q^n : d(\boldsymbol{r}, \boldsymbol{c}_o) = m \ \ \& \ \ d(\boldsymbol{r}, \boldsymbol{c}_i) \leq m \ \text{ for some } \ \boldsymbol{c}_i \in \mathcal{C} \setminus \boldsymbol{c}_o\}|$. Also, $(q-1)^m \binom{n}{m} = |\{\boldsymbol{r} \in F_q^n : d(\boldsymbol{r}, \boldsymbol{c}_o) = m\}|$. Since $(q-1)^{m_o-1} L(m_o-1) < (q-1)^{m_o-1} \binom{n}{m_o-1}$, then there exit words $\boldsymbol{r} \in F_q^n$ such that $\min_{\boldsymbol{c} \in \mathcal{C}} d(\boldsymbol{r}, \boldsymbol{c}) = m_o - 1$ and this minimum is achieved when $\boldsymbol{c}$ is the all zero codeword $\boldsymbol{c}_o$. By recalling that the covering radius is [11] $R_c = \max_{\boldsymbol{r} \in F_q^n} \min_{\boldsymbol{c} \in \mathcal{C}} d(\boldsymbol{r}, \boldsymbol{c})$, it follows that $R_c \geq m_o - 1$. ■

Corollary 4: For any linear (n,k) code $m_o \leq n-k+1$.

B. Sphere decoding of linear block codes on q-ary symmetric channels.

Let HSD$(m-1)$ denote a (hard decision) sphere decoder with radius $m-1$ that correctly decodes the received word if its Hamming distance from the transmitted word is less than m. Let $d(\boldsymbol{y}, \boldsymbol{v})$ be the Hamming distance between $\boldsymbol{y}$ and $\boldsymbol{v}$, then if $\boldsymbol{y} \in F_q^n$ is received, the output from the decoder is

$$\begin{aligned} \hat{\boldsymbol{c}} = \arg \min_{\boldsymbol{v} \in \mathcal{C}} \quad & d(\boldsymbol{y}, \boldsymbol{v}) \\ \text{subject to} \quad & d(\boldsymbol{y}, \boldsymbol{v}) < m. \end{aligned} \quad (5)$$

Using Gallager's bounding technique [12], the error plus failure probability of the sphere decoder, $P(\mathcal{E}_m)$, can be upper-bounded as follows

$$\begin{aligned} P(\mathcal{E}_m) &= P(\mathcal{E}_m, \zeta < r) + P(\mathcal{E}_m, \zeta \geq r) \\ &\leq \min_{r<m} \{P(\mathcal{E}_{ML}, \zeta < r) + P(\zeta \geq r)\}, \end{aligned} \quad (6)$$

which follows from the fact that the sphere decoder performs ML decoding within the specified search radius.

Theorem 5: The performance of HSD$(m-1)$ decoding of an (n,k,d) linear code, with a weight spectrum G_w, over a q-ary symmetric channel, with a success probability s and a crossover probability $p = (1-s)/(q-1)$, is upper bounded by

$$P(\mathcal{E}_m) \leq \begin{cases} P(\mathcal{E}_{ML}, \zeta < m_o) + P(\zeta \geq m_o), & m \geq m_o; \\ P(\mathcal{E}_{ML}, \zeta < m) + P(\zeta \geq m), & m < m_o, \end{cases}$$

where m_o is radius that minimizes (1) and is given by Th. 2. $P(\zeta \geq m)$ is given by (2) and $P(\mathcal{E}_{ML}, \zeta < m)$ is upper bounded by (3).

C. Numerical Examples

In Fig. 1, the binary image of the $(15,3)$ RS code is BPSK modulated over an AWGN channel. For 16-ary hard decisions, the channel is modelled as an QSC. The performance bound

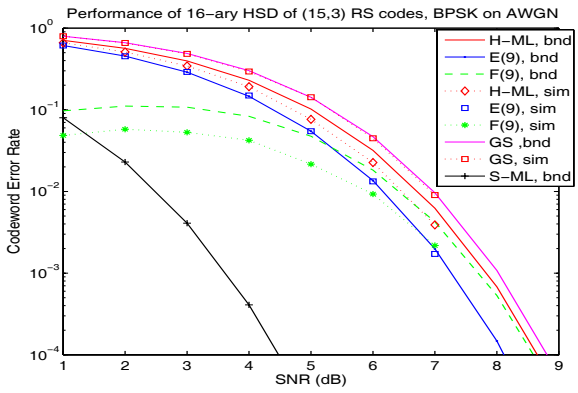

Fig. 1. The $(15, 3)$ RS code is BPSK modulated and transmitted over an AWGN channel. For the 16-ary hard-decision decoder, the channel is an QSC.

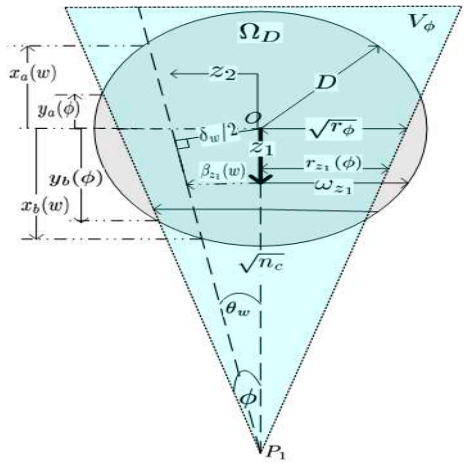

Fig. 2. The cone V_ϕ intersects the sphere Ω_D, $D > \sqrt{n_c}\sin(\phi)$.

of the hard ML (H-ML) decoder is shown (Th. 2) and is the same as an HSD of radius 9. The bounds of (2) and (3) are also shown and labeled as $F(9)$ and $E(9)$ respectively. As seen, the three bounds ('bnd') are in close agreement with the simulation ('sim'), for such a hypothetical sphere decoder. The error probability of the GS decoder with radius 8 is simulated and agrees with the bounded of Th. 5. For reference proposes, we show the average error probability of the soft decision bit level ML (S-ML) decoder (this is analyzed in [13]) which has about 4 dB gain over the symbol H-ML decoder.

III. Sphere Decoding Bounds for PSK Block Coded Modulation

Consider a sphere decoder when the modulation is M-ary or binary phase shift keying (PSK) [14] and each transmitted codeword in the code has the same energy when mapped to the PSK constellation. Complex sphere decoding algorithms which solve the closest point search problem were developed in [15]. We will derive a bound on the performance of the corresponding soft decision sphere decoder for BPSK modulation which is tighter than our previous bound [8]. We show how this bound is applied for the case of M-ary PSK modulation. We will assume that the modulated code is linear.

Note that the original code need not be binary. For example, an RS code defined over F_{2^m} could be mapped directly to an 2^m-ary PSK constellation by a one-to-one mapping from the symbols in F_{2^m} to the 2^m points in the PSK constellation.

We will introduce some notation, so the bound derived here is readily applicable for both BPSK and M-PSK modulation. Each codeword of length n will be mapped to a word of M-PSK symbols. If the code is binary, then each $\log_2(M)$ bits are mapped to an M-ary symbol. The number of channel symbols will be denoted by n_c; for a binary code of length n and M-PSK modulation, $n_c = n/\log_2(M)$ (For BPSK, $n_c = n$.) Let G_w be the number of codewords which are at an Euclidian distance δ_w from each other. For QPSK modulation and Gray encoding [14], $\delta_w = \sqrt{2w}$, where w is the (binary) Hamming distance between the codewords. For BPSK, $\delta_w = 2\sqrt{w}$. Let n_d denote the dimension of the considered space. For BPSK and M-PSK, $n_d = n_c$ and $n_d = 2n_c$ respectively. The code will have the property that all codewords are of equal energy and lie on a sphere of radius $\sqrt{n_c}$ from the origin of space.

Consider a soft decision sphere decoder with an Euclidean decoding radius D, SSD(D). Ω_D will denote an n_d dimensional sphere centered around the transmitted codeword (all zero codeword) while V_θ will denote an n_d dimensional right circular cone with half angle θ. Following Gallager's bounding technique and defining the region $\Lambda(\theta, D) \triangleq \{V_\theta \cap \Omega_D\}$ the error plus failure probability of SSD(D) is upper bounded by

$$P(\mathcal{E}_D) \leq \min_\theta \{P(\mathcal{E}_D|\boldsymbol{z} \in \Lambda(\theta, D))P(\boldsymbol{z} \in \Lambda(\theta, D)) + P(\boldsymbol{z} \notin \Lambda(\theta, D))\}, \quad (7)$$

where $\boldsymbol{z}$ is the n_d dimensional noise of variance σ^2.

The ML error probability for the case of BPSK and M-ary modulation is tightly upper bounded by the Poltyrev tangential sphere bound by [10], [16]

$$P(\mathcal{E}_{ML}) \leq P(\mathcal{E}_{ML}, \boldsymbol{z} \in V_\phi) + P(\boldsymbol{z} \notin V_\phi),$$

where $\tan(\phi) = \sqrt{r_\phi/n_c}$. By defining $\theta_b(r_o) \triangleq \cos^{-1}\left(\frac{\delta_b/2}{\sqrt{r_o(1-\delta_b^2/4n_c)}}\right)$, r_ϕ is the solution for r_o in this equation [16] $\sum_{b>0} G'_b(r_o)\int_0^{\theta_b(r_o)} \sin^{n_d-3}(\vartheta)\mathrm{d}\vartheta = \frac{\sqrt{\pi}\Gamma(\frac{n_d-2}{2})}{\Gamma(\frac{n_d-1}{2})}$. $G'_b(r_o)$ is equal to G_b if $\delta_b^2/4 < r_o(1-\delta_b^2/4n_c)$ and is zero otherwise. From (7), one can prove the following theorem.

Theorem 6: The performance of SSD(D) for BPSK or MPSK modulation is upper bounded by

$$P(\mathcal{E}_D) \leq \begin{cases} P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_D) + P(\boldsymbol{z} \notin \Omega_D), & D \leq \sqrt{n_c}\sin(\phi); \\ P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Lambda(\phi, D)) + P(\boldsymbol{z} \notin \Omega_D) + \\ P\left(\{\boldsymbol{z} \notin V_\phi\} \cap \{\boldsymbol{z} \in \Omega_D\}\right), & D > \sqrt{n_c}\sin(\phi) \end{cases}.$$

We will call $D_\phi = \sqrt{n_c}\sin(\phi)$ the critical decoding radius. We will now give expressions for the different terms that appeared in the theorem;

$$P(\boldsymbol{z} \notin \Omega_D) = 1 - \Gamma_r(n_d/2, D^2/2\sigma^2), \quad (8)$$

where the regularized Gamma function Γ_r is given in terms of the Gamma function Γ by

$$\Gamma_r(v/2, w/2) = \begin{cases} \int_0^w \frac{t^{v/2-1}e^{-t/2}}{2^{v/2}\Gamma(v/2)}\mathrm{d}t, & w \geq 0; \\ 0, & w < 0. \end{cases} . \quad (9)$$

The joint probability of an ML error and $\boldsymbol{z} \in \Omega_D$ is

$$P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_D) = \sum_{b:\, 0<\delta_b/2<D} G_b \int_{\sqrt{b}}^{D} \mathcal{N}(z_o)\Gamma_r\left(\frac{n_d-1}{2}, \frac{D^2-z_o^2}{2\sigma^2}\right)\mathrm{d}z_o, \quad (10)$$

where $\mathcal{N}(z) = \frac{1}{\sqrt{2\pi\sigma^2}}e^{-z^2/2\sigma^2}$ is the normal distribution.

Define $y_a(\phi)$ and $y_b(\phi)$ to be the altitudes at which the cone V_ϕ intersects the sphere Ω_D (see Fig. 2).. It follows that $y_{a,b}(\phi) = \sqrt{n_c}(1 - 2U_{a,b}(\phi, D))$, where $U_{a,b}(\theta, D) = \frac{4n_c \pm \sqrt{16{n_c}^2 - 16n_c\sec^2(\theta)(n_c - D^2)}}{8n_c\sec^2(\theta)}$. The cone V_ϕ intersects Ω_D if $D > \sqrt{n_c}\sin(\phi)$ at which

$$P\left(\{\boldsymbol{z} \notin V_\phi\} \cap \{\boldsymbol{z} \in \Omega_D\}\right) = \int_{y_a(\phi)}^{y_b(\phi)} \mathcal{N}(z_1) \left[\Gamma_r\left(\frac{n_d-1}{2}, \frac{\omega_{z_1}^2}{2\sigma^2}\right) - \Gamma_r\left(\frac{n_d-1}{2}, \frac{r_{z_1}^2(\phi)}{2\sigma^2}\right)\right]\mathcal{N}(z_1)\mathrm{d}z_1,$$

where $\omega_{z_1}^2 = D^2 - z_1^2$ and $r_{z_1}(\phi) \triangleq \sqrt{r_\phi}\left(1 - \frac{z_1}{\sqrt{n_c}}\right)$. Consider a codeword at a distance δ_w, then the half angle of the cone bisecting this distance is $\theta_w = \sin^{-1}(\delta_w/2\sqrt{n_c})$. This cone will intersect the sphere Ω_D at altitudes $x_a(w)$ and $x_b(w)$ given by $x_{a,b}(w) = \sqrt{n_c}(1 - 2U_{a,b}(\theta_w, D))$. Let $\beta_{z_1}(w) \triangleq \frac{\sqrt{n_c} - z_1}{\sqrt{\frac{4n_c}{\delta_w^2} - 1}}$. Now define the integrals

$$\mathcal{I}(\gamma, w, z_1) \triangleq \mathcal{N}(z_1)\int_{\beta_{z_1}(w)}^{\gamma} \mathcal{N}(z_2)\Gamma_r\left(\frac{n_d-2}{2}, \frac{\gamma^2 - z_2^2}{2\sigma^2}\right)\mathrm{d}z_2,$$

and

$$\mathcal{I}_2(w) = \int_{x_a(w)}^{y_a(\phi)} \mathcal{I}(\omega_{z_1}, w, z_1)\mathrm{d}z_1 + \int_{y_a(\phi)}^{y_b(\phi)} \mathcal{I}(r_{z_1}(\phi), w, z_1)\mathrm{d}z_1 + \int_{y_b(\phi)}^{x_b(w)} \mathcal{I}(\omega_{z_1}, w, z_1)\mathrm{d}z_1.$$

Taking the union over all the non-zero Euclidean weights, it follows that for $D > \sqrt{n_c}\sin(\phi)$,

$$P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Lambda(\phi, D)) = \sum_{w>0} G'_w(r_\phi)\mathcal{I}_2(w). \quad (11)$$

It is to be noted that the same equations hold whether $D > \sqrt{n_c}$ or $\sqrt{n_c}\sin(\phi) < D \leq \sqrt{n_c}$.

In Fig. 3, we show how the bounds derived for M-ary modulated spherical codes are tight. A codeword in the $(24, 12)$ Golay code is mapped into 12 QPSK symbols and transmitted over AWGN channel. As observed, the simulated performance of the ML decoder and the SD sphere decoder are tightly bounded by the bounds given in this section. The critical decoding radius in the 2×12 dimensional space is $D_\phi = 2.667$.

IV. Sphere Decoding of Finite Lattices

In this section, we consider the case of soft decision sphere decoding of a general finite lattice or code $\mathcal{C}$. The code is not constrained to be a linear code and the transmitted codewords are not constrained to have a fixed energy The channel symbols of a transmitted codeword are also not required to have the same energy. Define $G_w(i)$ to be the number of mapped codewords with an Euclidean distance δ_w from the ith codeword. Given that $\boldsymbol{c}_i$ is transmitted, let the error probability of SSD(D) be upper bounded by $P_i(\mathcal{E}_D)$. By taking the expectation over all codewords,

$$P(\mathcal{E}_D) \leq \frac{1}{|\mathcal{C}|}\sum_{\boldsymbol{c}_i \in \mathcal{C}} P_i(\mathcal{E}_D). \quad (12)$$

Now, if we assume that $P_i(\mathcal{E}_D)$ is of the union bound form; $P_i(\mathcal{E}_D) = \sum_{w>0} G_w(i)P_i^{(w)}(\mathcal{E}_D)$, where $P_i^{(w)}(\mathcal{E}_D)$ is the probability of a sphere decoder error due to incorrectly decoding a codeword at a distance δ_w when $\boldsymbol{c}_i$ is transmitted. The error probability of SSD(D) can thus be upper bounded by $P(\mathcal{E}_D) \leq \sum_{w:\, \delta_w>0} \bar{G}_w P^{(w)}(\mathcal{E}_D)$, where $P^{(w)}(\mathcal{E}_D)$ is the probability that the sphere decoder erroneously decodes a codeword at a distance w from the transmitted codeword and

$$\bar{G}_w = \frac{1}{|\mathcal{C}|}\sum_{\boldsymbol{c}_i \in \mathcal{C}} G_w(i), \quad (13)$$

is the average number of codewords which are at an Euclidean distance δ_w from another codeword. The ML error probability was analyzed for such a case by Hughes [17], [18]. The optimum radius that minimizes the Hughes upper bound on the ML error probability will be denoted by D_o.

Theorem 7: The error (plus failure) probability of SSD(D) of an arbitrary finite lattice or code is upper bounded by

$$P(\mathcal{E}_D) \leq \begin{cases} P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_D) + P(\boldsymbol{z} \notin \Omega_D), & D < D_o; \\ P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_{D_o}) + P(\boldsymbol{z} \notin \Omega_{D_o}), & D \geq D_o. \end{cases},$$

where D_o is the root of the equation

$$\sum_{w:\, 0<\frac{\delta_w}{2}<D} \bar{G}_w \int_0^{\theta_{w,D}} \sin(\theta)^{n_d-2}\mathrm{d}\theta = \frac{\sqrt{\pi}\Gamma\left(\frac{n_d-1}{2}\right)}{\Gamma\left(\frac{n_d}{2}\right)}, \quad (14)$$

and $\theta_{w,d} = \cos^{-1}(\delta_w/2D)$.

The theorem follows by observing that SSD(D) is equivalent to the maximum likelihood decoder if the received word falls within an Euclidean distance D from the transmitted one.

The bound developed here is universal in the sense that also applies for the case of a linear code with equal energy codewords. However, it is to be noted that the Hughes bound on ML decoding is not tighter than the Poltyrev tangential sphere bound [19] which implies that for MPSK and BPSK modulated schemes the bound of Th. 6 is tighter than that of Th. 7.

For the case of M-PSK modulation of a linear code, the constellation may not result in a Hamming space if $M > 4$. In such a case the ensemble average weight enumerator $\bar{G}_w$ (13) can be used with the bounds of Sec. III to analyze the performance. The same technique can be used with the results in Sec. II for general nonlinear lattices transmitted over q-ary symmetric channels.

A. Numerical Example

Assume an $(15, 3)$ RS code over F_{16} and assume a one-to-one mapping from the symbols of F_{16} to the points of an 16-QAM modulation [14], whose average energy per symbol is 10. The resulting lattice is no longer linear, meaning that it

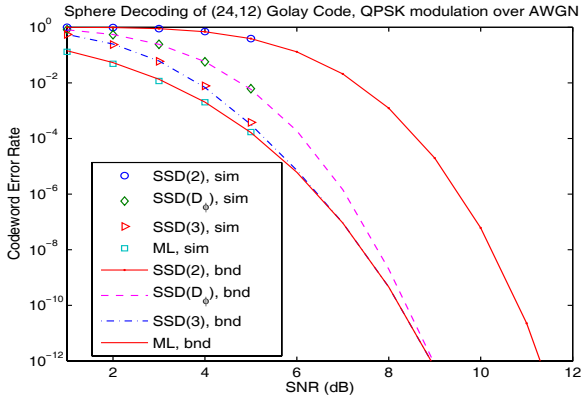

Fig. 3. Bounds on the performance of soft-decision sphere decoding of the $(24, 12)$ Golay code when QPSK modulated over an AWGN channel.

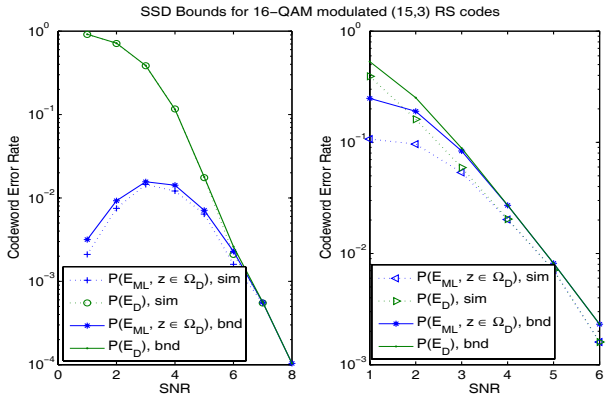

Fig. 4. The $(15, 3)$ RS code is 16-QAM modulated and transmitted over an AWGN channel. The sphere decoder is a soft decision sphere decoder with an Euclidean radius 10 (left) and $D_o = 12.9$ (right). The bounds are compared to simulations for a sphere decoding ML error and the error plus failure probability.

is not necessary that $G_w(\boldsymbol{c}_i) = G_w(\boldsymbol{c}_j)$ if $i \neq j$. Furthermore, the codewords (lattice points) are not of equal energy. The ensemble weight enumerator $\bar{G}_w$ was numerically computed to evaluate the bounds. The radius that minimizes the bound on the ML error probability is $D_o = 12.9$. In Fig. 4, we confirm that the bounds on the sphere decoder error probability agree with the simulations for the cases of $D = 10$ and $D = D_o$. We also compare the simulated performance of ML error probability $P(\mathcal{E}_{ML}, \boldsymbol{z} \in \Omega_D)$ to that of the analytic performance in both cases. At low SNRs this probability is low as the probability of the received word falling inside the sphere is relatively low. As more received words fall inside the sphere, the ML error probability increases as the SNR increases. At a certain SNR, the probability of the ML error starts decreasing due to the improved reliability of the received word.

V. Conclusions

Bounds on the error plus failure probability of hard-decision and soft-decision sphere decoding of block codes were derived. By comparing with the simulations of the corresponding decoders these bounds are tight. The ML performance of codes on q-ary symmetric channels is analyzed. The performance of sphere decoding of Reed Solomon codes and their binary images was analyzed. Moreover, the bounds are extremely useful in predicting the performance of the sphere decoders at the tail of error probability when simulations are prohibitive. The bounds allows one to pick the radius of the sphere decoder that fits best the performance, throughput and complexity requirements of the system.

Acknowledgment

This research was supported by NSF grant no. CCF-0514881 and grants from Sony, Qualcomm, and the Lee Center for Advanced Networking.

References

[1] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of Computation*, vol. 44, pp. 463–471, Apr. 1985.
[2] E. Agrell, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.
[3] C. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Programming*, vol. 66, pp. 181–191, 1994.
[4] E. Viterbo and J. Boutros, "A universal lattice decoder for fading channels," *IEEE Trans. Inform. Theory*, vol. 45, p. 1639.
[5] H. Vikalo and B. Hassibi, "On joint detection and decoding of linear block codes on gaussian vector channels."
[6] M. O. Damen, H. E. Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, p. 2389, 2003.
[7] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon codes and algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.
[8] M. El-Khamy, H. Vikalo, and B. Hassibi, "Bounds on the performance of sphere decoding of linear block codes," in *Proc. of IEEE Information Theory Workshop on Coding and Complexity, ITW2005, Rotorua, New Zealand*, 2005.
[9] R. J. McEliece and L. Swanson, "On the decoder error probability of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 5, pp. 701–703, Sep. 1986.
[10] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.
[11] F. J. MacWilliams and N. J. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North Holland, 1977.
[12] I. Sason and S. Shamai, "Performance analysis of linear codes under maximum-likelihood decoding: a tutorial," submitted to *Foundations and Trends in Communications and Information Theory*, NOW Publishers, Delft, the Netherlands.
[13] M. El-Khamy and R. J. McEliece, "Bounds on the average binary minimum distance and the maximum likelihood performance of Reed Solomon codes," in *42nd Allerton Conf. on Communication, Control and Computing*, 2004.
[14] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2001.
[15] Hochwald and S. ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Commun.*, vol. 53, pp. 389–399, March 2003.
[16] H. Herzberg and G. Poltyrev, "The error probability of M-ary PSK block coded modulation schemes," *IEEE Trans. Commun.*, vol. 44, no. 4, pp. 427–433, April 1996.
[17] B. Hughes, "On the error probability of signals in additive white Gaussian noise," *IEEE Trans. Inform. Theory*, pp. 151–155, Jan 1991.
[18] H. Herzberg and G.Poltyrev, "Techniques of bounding the probability of decoding error for block coded modulation structures," *IEEE Trans. Inform. Theory*, pp. 903–911, May 1994.
[19] D. Divsalar, "A simple tight bound on error probability of block codes with application to turbo codes," TMO Progress Report, NASA,JPL, Tech. Rep. 42–139, 1999.